THE CHURCH OF ENGLAND

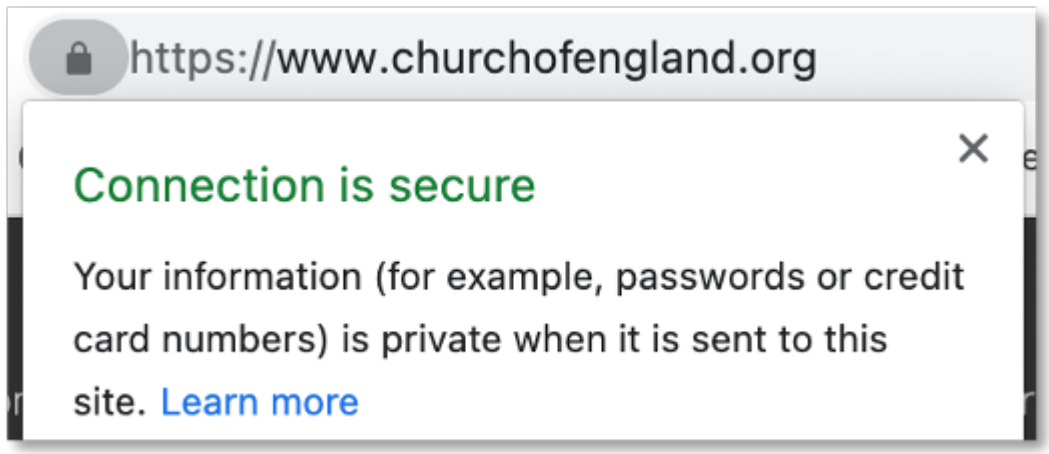
An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic. It's not just an important bit of tech, but a sign that your website is secured and can be trusted.

If you're looking for a technical explanation of SSL (Secure Sockets Layer) certificates and the technology behind it, it's probably best to read a blog like this from Cloudflare. Our blog is primarily about why you should have an SSL certificate on your church's website.

We'll be linking to descriptions of various web technologies on the Cloudflare website during this blog if you want to understand more about them.

What is an SSL certificate?

SSL is a set of rules for encrypting internet traffic and verifying the identity of a website. An SSL certificate is what enables a website to move from HTTP to HTTPS, which is more secure. From a user perspective, it's predominantly the difference between seeing a locked padlock next to your website URL in the browser (encrypted) or an unlocked padlock (unsecure).

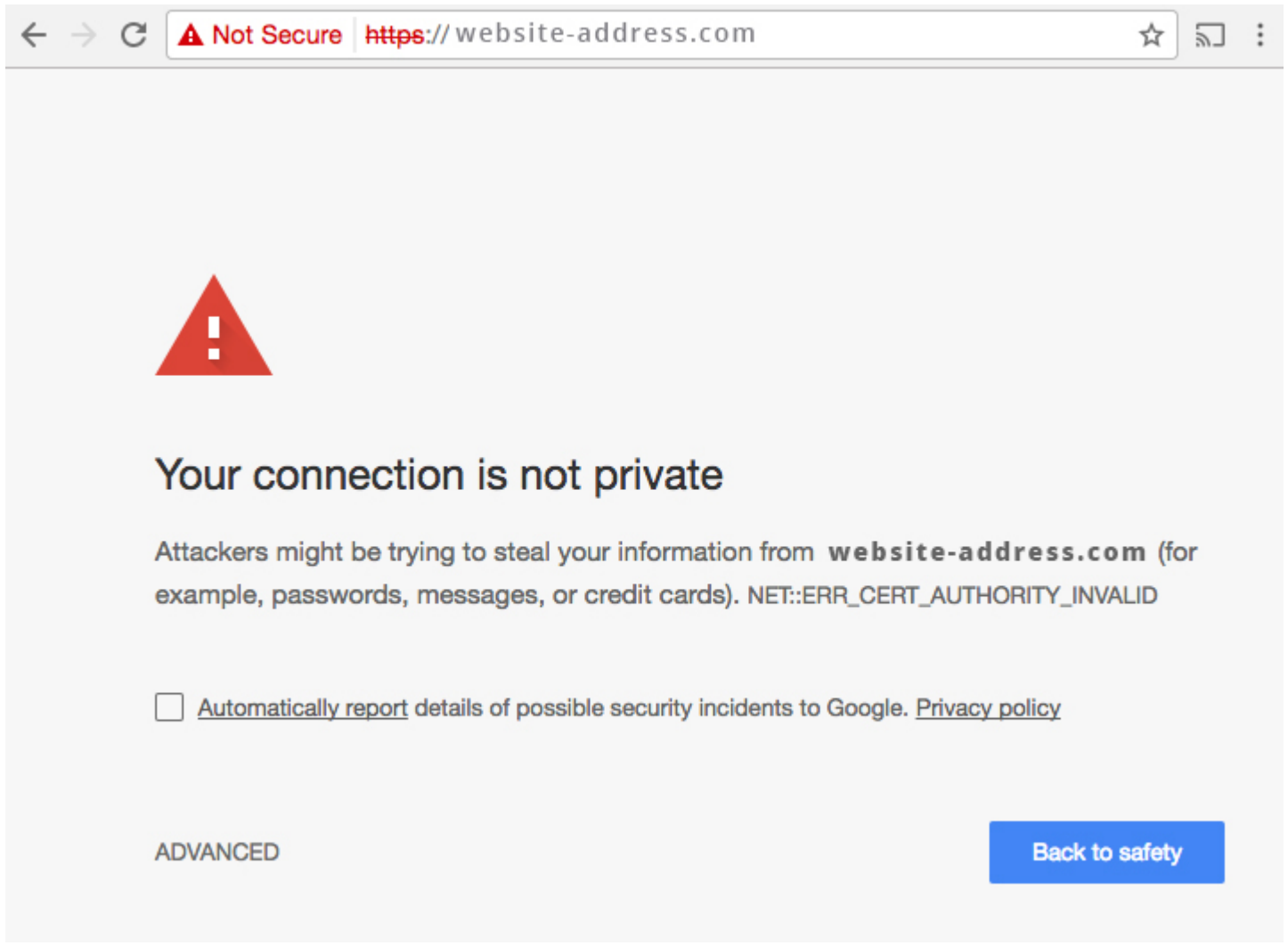


This image shows that the website **www.churchofengland.org** has a secured connection, which means that any data transmitted over the website is encrypted. This builds trust with website visitors and stops the website from being negatively flagged in search results.

A website needs an SSL certificate in order to:

- keep user data secure
- verify ownership of the website
- prevent attackers from creating a fake version of the site
- gain user trust.

That final point is becoming more and more important each day. While we've all relied on the technology behind websites to achieve the first three bullets, gaining user trust is something we should actively be managing. In fact, Google now actively flags websites that do not have an SSL certificate and warns users about visiting them before letting them pass through from their search results page. The alert can look different depending on which browser you use, but the below example shows what clicking on an unsecure website link in Google Chrome looks like:



After clicking on this website link, Google Chrome displays a warning message to the user about visiting the unsecure website. To visit the website, users must click on 'Advanced' before being able to continue through.

How do I get an SSL certificate?

This is where things can get a bit complicated because you can obtain an SSL certificate in a number of different ways. The two easiest ways are via:

1. The web company you use to host your website
2. A third party company who supply SSL certificates that you need to manage

If you host your website directly with a hosting company or via a web agency, you can ask them to implement an SSL certificate on your domain, usually for a small annual fee. This is by far the easiest way of ensuring that the certificate is valid, stays up to date and is working correctly. You shouldn't have to pay a huge amount for this service and it's often sensible to allow the experts manage this on your behalf!

If you are involved in maintaining your website hosting and have access to the control panel for your domain and hosting, you might be able to issue and maintain an SSL certificate yourself from a third party. While this is usually a free service, the certificates tend to only be valid for three months at a time and require you to re-issue them every three months. **We'd only recommend using this method if you are comfortable with**

domain management and understand the risk of not re-issuing an SSL certificate if you miss a renewal date. If you'd like to learn more about issuing an SSL certificate from a non-profit Certificate Authority, there are two suppliers listed below:

- Let's Encrypt
- SSL For Free

Do I really need one?

You don't accept donations on your website, you don't have user accounts where people store personal data and you're not asking people to sign up to newsletters - so do you really need an SSL certificate?

The answer is yes - if only because it shows search engines like Google and Bing that you're website has been verified, is on an encrypted platform and can be trusted. If you're operating any of the above extra pieces of functionality on your website, you should be implementing an SSL certificate as a priority.

Security online is only going to become a more important and vital step in securing online platforms in the future.

What other options do I have?

If maintaining a separate church website is something that seems to be costing too much or you don't have the time to take care of, we've made it possible for you to turn your A Church Near You church page into a mini-website. The great thing about this is that we take care of all the security updates, platform improvements, bug fixes and the SSL certificate!

If you want to find out more about using the **A Church Near You** website as your own church website, you can read more in this support article .

Ben Hollebon

Web and Insights Manager

Keep up to date with all things digital and join our Digital Labs newsletter

Subscribe here

- ## How to Design a Church Logo, Even If You're Not a Designer

01/05/2024

- ## Images and copyright: A guide to using images online legally

19/04/2024

- ## How to make the most of Instagram to reach your audience in 2024

12/04/2024